

PAT-NO: JP406195361A  
DOCUMENT-IDENTIFIER: JP 06195361 A  
TITLE: ELECTRONIC VOTING DEVICE  
PUBN-DATE: July 15, 1994

INVENTOR-INFORMATION:

NAME

SAKO, KAZUE

MASUMOTO, HIROYUKI

ASSIGNEE-INFORMATION:

NAME

NEC CORP

COUNTRY

N/A

APPL-NO: JP04292854

APPL-DATE: October 30, 1992

INT-CL (IPC): G06F015/28

ABSTRACT:

PURPOSE: To provide the electronic voting device which can enable voting without signature in an electronic network and further can prevent illegal voting by providing a key certifying means for an election manager while allocating signature certificate keys and signature secret keys to voting persons.

CONSTITUTION: This non-signature electronic voting system is composed of a preparation phase, tag vote generation phase, voting phase and result open phase. First of all, an election managing center 100 sets a quorum for signature and presents the quorum for signature on an electronic bulletin board 102. The voting person reads the information written on the bulletin

board 102  
by using a bulletin board reading means 301, prepares a tag vote (t)  
by using a  
tag vote preparing means 310, simultaneously prepares a voting person  
signature  
secret key (d) and holds it by a signature key holder 312. The  
center 100  
transmits a blind signature D to the elector preparing the tag vote  
by using a  
blind signature transmitting means 205. A signature preparing means  
306  
prepares a signature sentence T of the tag vote (t) to be certified  
by the open  
key of the center while using the signature D sent from the center  
100 and the  
quorum for certificate.

COPYRIGHT: (C)1994,JPO&Japio



## 【特許請求の範囲】

【請求項1】 投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施す署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする電子投票装置。

【請求項2】 投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施す署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を暗号化して無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする電子投票装置。

【請求項3】 投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵と投票内容に依存したビット列に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施す署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする電子投票装置。

【請求項4】 投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵と投票内容に依存したビット列に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施す署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を暗号化して無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする電子投票装置。

【請求項5】 請求項1又は3の電子投票装置において、選挙管理者が無記名で送付された投票文を一方向性関数で変換して公開する公開手段を有することを特徴とする電子投票装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は電子ネットワーク上で有権者だけが1度だけ無記名で投票でき、投票者が自分が何に投票したかを他の投票者に知られることなく不正集計に対して異議申し立てをオープンにできる方式において、同一投票者が2つ以上の選択肢に投票することを検出でき、かつこの検出機構を第三者に悪用されない装置を提案することを目的とする。

## 【0002】

【従来の技術】電子投票方法として従来から知られているものは太田の方法がある。これは特開平1-177164号及び昭和63年電子情報通信学会春季全国大会A-294「単一の選挙管理者を用いた電子投票方式」に開示されている。この方式は投票者は乱数で変換した投票内容に対してセンタの署名を得た後、投票者側で乱数成分を取り除いたもとの投票内容に対するセンタの署名を作成し、これを無記名でセンタに送ることにより無記名投票を実現している。各投票者は自分の投票が受理・集計されたことを、センタが発表する投票内容一覧で確認する。この方法では自分の意見を反映させた投票内容に対してのみセンタの署名を得られるので、センタがその投票内容を集計しなかった場合、自分の投票内容を公開して異議申し立てを行わなくてはならない。

【0003】この問題を解決すべく、異議申し立てを行なう場合も、投票者が自分の投票内容を公開せずに異議申し立てを行なうために、あらかじめ投票内容に依存しない投票用紙にのみ署名をもらい、署名付きの投票用紙に自分の意見を反映させた投票内容をセンタに送るという方式が、特願平4-108069号で示された。実施例として各有権者は賛成票・反対票及び投票タグからなる署名つき投票用紙を記名式で入手し、そのうち一方の票を投票タグと共に無記名で投票する方式が述べられている。さらに、不正投票者が2つ以上の意見に投票することを防ぐことを考えた電子投票ほうしきが特願平4-222580号で示された。実施例として投票タグを投票者が生成した署名検証鍵として、各投票者は対応する署名秘密鍵で署名された賛成票・反対票及び投票タグからなる署名つき投票用紙を記名式で入手し、そのうち一方の票を投票タグと共に無記名で投票する方式が述べられている。

【0004】また、1992年電子情報通信学会秋季大会においてA-188「実用的かつ安全な無記名投票方式」が発表された。これは公平性を追及するため、投票者が二度にわたって匿名通信を行う方式である。

## 【0005】

【発明が解決しようとする課題】特願平4-108069号や特願平4-222580号において、投票用紙の情報量は投票の選択肢の数に比例して大きくなるという問題点がある。たとえば、賛成・反対の2値の投票を行

なう場合には投票用紙は賛成票・反対票・タグ票からなるが、賛成・反対・保留の3値の投票を行なう場合には投票用紙は賛成票・反対票・保留票・タグ票としなくてはならないように、選択肢が増えるにしたがって通信量や処理量が増加する。さらに、あらかじめ選択肢が固定されていないと投票用紙を作成できず、自由記入形式の投票やアンケートや意見書に対応できないという問題点があった。

【0006】本発明では選択肢の数が増えても、また選択肢があらかじめ固定されていなくても投票者が1回の匿名通信を用いて効率よく実現できる電子投票装置を提案する。

【0007】

【課題を解決するための手段】第一の発明の電子投票装置は、投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施す署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする。

【0008】第二の発明の電子投票装置は、投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施す署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を暗号化して無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする。

【0009】第三の発明の電子投票装置は、投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵と投票内容に依存したビット列に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施す署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする。

【0010】第四の発明の電子投票装置は、投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵と投票内容に依存したビット列に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施す署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を暗号化して無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする。

【0011】第五の発明の電子投票装置は、請求項1又

は3の電子投票装置において、選挙管理者が無記名で送付された投票文を一方方向関数で変換して公開する公開手段を有することを特徴とする。

【0012】

【実施例】つぎに、図1から図8を参照して第一、第二、第三、第四及び第五の発明の実施例について説明する。

【0013】本発明の電子投票装置を、図2のように、 $m$ 個の投票者サブシステム101(1)～101( $m$ )及び1つの選挙管理センタ100が相互に安全な通信チャネル(例えばデータ回線)105で結ばれており、さらに選挙管理センタ100のみが書き込み可能な掲示板で、すべての投票者サブシステムが読み出せる電子掲示板102が存在する場合の無記名電子投票システムに実施する例を述べる。なお、以下簡単のために選挙管理センタをセンタ、投票者サブシステムを投票者と呼ぶことにする。

【0014】この投票システムは準備フェーズと、タグ票生成フェーズ、投票フェーズおよび結果公表フェーズからなる。

【0015】第一及び第三の発明はタグ票生成フェーズ、第二及び第四の発明は投票フェーズ、第五の発明は結果公表フェーズに関する。

【0016】まず、図3を用いて第一の発明の準備フェーズを説明する。

【0017】本無記名電子投票システムを実施するための準備として、センタ100は署名用の定数を設定し、検証用定数を電子掲示板102に掲示する。例えば、署名方式としてRSA暗号方式を用いるとする。そこで、 $n_c$ を二つの素数 $p_c$ 、 $q_c$ の積とし、 $e_c$ と $d_c$ を $e_c \cdot d_c = 1 \bmod (p_c - 1)(q_c - 1)$ を満たす整数とする。このときセンタは $e_c$ 、 $n_c$ を検証用定数として設定する(ステップ11)。これらの定数を電子掲示板102に書き込む(ステップ12)。今後この検証用定数 $e_c$ 、 $n_c$ は頻繁に用いられるので自分の定数保持手段201に書き込み容易にアクセスできるようにする(ステップ13)。一方、 $d_c$ は自分の秘密情報保持手段202に格納する(ステップ14)。

【0018】次に、センタ100は投票に関する規則を定める。まず、投票対象の議題を明らかにする。次に投票フォーマットとしてタグ票フォーマットと投票内容フォーマットを定める。たとえば、以下のようなタグ票フォーマットを考える。このとき、 $e$ と $n$ と

【0019】

ハッシュ値 $h(e \parallel n)$

【0020】の連結で、数字として $n_c$ より小さくなるようなものをタグ票とする。たとえば、関数 $h$ の出力を64ビット、 $e$ を10ビット、 $n$ を512ビットと定め、あらかじめ $n_c$ を587ビットに設定すればよい。

【0021】また、投票内容フォーマットとしては以下

5

が考えられる。投票内容 $x$ と乱数 $y$ を連結した  
【0022】

$$x||y$$

【0023】と、その

【0024】

$$\text{ハッシュ値}h(e||n)$$

【0025】を連結したもの

【0026】

$$x||y||h(x||y)$$

【0027】とする。このとき、投票内容全体として $n$ より小さいものとする。投票内容 $x$ はあらかじめ付与された選択肢番号でもいいし、自由形式に記述した文章をアスキー文字列に置き換えたものでもよい(ステップ15)。

【0028】次に、投票する権利のあるサブシステム(以後、有権者と呼ぶ)の名前を一覧にする(ステップ16)。投票用紙作成及び投票の期限を設定・公表し(ステップ17)、タグ票作成フェーズの開始を合図する(ステップ18)。

【0029】以上が準備フェーズである。

【0030】次に、タグ票作成フェーズ、及び投票フェーズを説明するが、両フェーズとも選挙管理センタ100は各投票者に対して同じ手順を踏むので、特定の投票者サブシステム101(i)に対する手順を例にとって説明を続ける。

【0031】図1に示すように無記名電子投票システムはセンタ100が電子掲示板102に定数及び投票規則を書き込む安全通信チャネル103、投票者101(i)が電子掲示板102に書かれた内容を読み出すための安全通信チャネル104(i)および投票者とセンタが通信するための安全通信チャネル105(i)で構成されている。

【0032】まず、図1を参照しながら投票者101(i)のタグ票作成フェーズを説明する。投票者101(i)は掲示板読み出し手段301を用いて掲示板102に書かれてある内容を読み出し、定数 $e_c$ 、 $n_c$ を定数保持手段302に格納する一方、読み出したフォーマットに沿うようなタグ票 $t$ をタグ票作成手段310にて作成する。すなわち、まず2つの素数 $p$ 、 $q$ の積である512ビットの数 $n$ を定め、 $(p-1)(q-1)$ と互いに素な10ビットの数 $e$ をさだめる。これと

【0033】

$$h(e||n)$$

【0034】を連結させたものをタグ票 $t$ とする。すなわち

【0035】

$$t=e||n||h(e||n)$$

【0036】とする。また、同時に

$$e \cdot d = 1 \pmod{(p-1)(q-1)}$$

となる $d$ を求め、投票者署名秘密鍵として保持する。な

6

お、タグ票作成にあたってフォーマットに必要な乱数成分は乱数発生器303の出力を用いる。

【0037】次に、タグ票変換器304は、乱数発生器303の出力 $r$ と定数 $e_c$ 、 $n_c$ を用いて、

【0038】

$$s=t \cdot r^{e_c} \pmod{n_c}$$

【0039】を計算し、 $s$ を出力する。また、このときの乱数発生器303の出力 $r$ は乱数保持器309に格納する。 $s$ を記名付き送信手段305が安全チャネル105(i)を通じてセンタ100に送信する。

【0040】センタ100はタグ票受信手段206で受信した正当な有権者からの $s$ を受信する。ブラインド署名生成器204は秘密保持手段201、定数保持手段202から読み出した $d_c$ 及び $n_c$ を用いて、

【0041】

$$D=s^{d_c} \pmod{n_c}$$

【0042】を計算し、出力する。ブラインド署名送信手段205は $D$ を投票者101(i)に送信する。

【0043】タグ票作成を行なったすべての有権者に対して署名を送信すればセンタは投票フェーズに移行することを宣言する。以上がタグ票設定フェーズである。

【0044】次に、投票フェーズを説明する。

【0045】署名作成手段306は、ブラインド署名受信手段311によりセンタ100から受信した $D$ と、定数保持手段302から読み出した $e_c$ 、 $n_c$ を用いて

【0046】

$$s=D^{e_c} \pmod{n_c}$$

【0047】が成立するかどうか検証する。確認できれば、乱数保持器309から読み出した整数 $r$ と、定数保持手段302から読み出した $n_c$ 、 $e_c$ を用いて、

$$T=D/r \pmod{n_c}$$

を計算する。

【0048】なお、この $T$ はセンタの公開鍵 $e_c$ 、 $n_c$ で検証可能なタグ票 $t$ の署名文になっている。すなわち、

【0049】

$$T^{e_c} \pmod{n_c} = t$$

【0050】がなりたっている。センタにはタグ票 $t$ そのものを見せずにその署名を入手することをブラインド署名と呼び、一連のタグ票変換器304、ブラインド署名生成器204、署名作成手段306がタグ票認証手段である。なお、タグ票は投票者の署名検証鍵でもあるので、鍵認証手段でもある。

【0051】次に、投票文作成器307において投票文を作成する。まず、投票内容フォーマットに従い、自分の投票内容 $x$ を反映させた投票 $v$ を以下のように生成する。

【0052】

$$v=x||y||h(x||y)$$

【0053】ここで $y$ は発生器303の出力である。次

7

に署名鍵保持器から読み出した署名鍵 $d$ を用いて $v$ に署名を施す。すなわち、

$$v' = v^d \bmod n$$

を計算する。無記名送信手段308はこの署名とブラインド署名で得たタグの署名の対 $v = (v', T)$ を送信者名を付記せずにセンタ100に送出する。

【0054】センタ100は、受信した $V$ のうち $T$ を読み出し

【0055】

$$\alpha = t^{e_c} \bmod n_c$$

【0056】を計算する。 $\alpha$ は投票者が不正をしていなければ、 $t$ に等しくなる。 $\alpha$ があらかじめ定められたタグのフォーマットであれば、これと同じタグ票が以前使われているかどうか検証する。使われていなければ、次に投票内容を検証する。すなわち、タグ票から署名検証鍵 $e, n$ を抽出し、

$$\beta = (v')^e \bmod n$$

を計算する。 $\beta$ は投票者が不正をしていなければ、 $v$ に等しくなる。 $\beta$ があらかじめ定められた投票内容のフォーマットであれば、これから $x$ を抽出し、これを集計する。

【0057】全員の投票が終了したら、センタは結果を公表する。すなわち、すべてのタグ票と投票文の一覧を掲示板に掲げる。各投票者はその一覧を見て、自分の投票が集計されたかどうかを見ることができる。もし集計されていなければ、集計されていないタグ票を公表することにより、センタの集計洩れを指摘でき、かつこの時他の投票者には自分が何に投票したか知られることはない。

【0058】次に図5を用いて第二の発明の実施例を説明する。準備フェーズとして、第一の発明の実施例の準備フェーズと同様に行なうが、ステップ11において、センタはさらにRSA暗号鍵 $n_2, e_2, d_2$ を生成し、ステップ12において公開鍵 $e_2, n_2$ を掲示すると共にステップ13において $d_2$ を自分の定数保持手段201に書き込むところが付加される。

【0059】また、タグ票作成フェーズも第一の発明の実施例と同様に行なうが、掲示板読み出し手段401において $e_2, n_2$ の読み出し、格納が付加される。

【0060】投票フェーズも第一の発明の実施例と同様に行なうが、投票フェーズにおいて投票文作成器の出力 $V = (v', T)$ を入力とした投票文暗号化器407をおく。この投票文暗号化器においては、投票文 $V$ を以下のように暗号化する。定数保持手段302から読み出した $n_2, e_2$ を用いて、

【0061】

$$V' = (v', T^{e_2} \bmod n_2)$$

【0062】を計算し、無記名送信手段408は $V' = (v', T')$ を送信者名を付記せずにセンタ100に

8

送出する。

【0063】センタ100は、受理票検証手段417において、受信した $V'$ のうち $T'$ を読み出し

【0064】

$$\alpha = (T')^{d_2} \bmod n_2^{e_2} \bmod n_c$$

【0065】を計算する。 $\alpha$ は投票者が不正をしていなければ、 $t$ に等しくなる。 $\alpha$ があらかじめ定められたタグのフォーマットであれば、これと同じタグ票が以前使われているかどうか検証する。使われていなければ、次に投票内容を検証する。すなわち、タグ票から署名検証鍵 $e, n$ を抽出し、

$$\beta = (v')^e \bmod n$$

を計算する。 $\beta$ は投票者が不正をしていなければ、 $v$ に等しくなる。 $\beta$ があらかじめ定められた投票内容のフォーマットであれば、これから $x$ を抽出し、これを集計する。

【0066】公表手段としては、暗号化したままの $V'$ を掲示し、各自自分の投票文が集計されているかどうかを検証すればよい。

20 【0067】なお、投票文暗号化器407における投票文の暗号化方法としては、上記以外に $v$ を暗号化する、 $v'$ を暗号化する、あるいは投票文とタグ票のどちらも暗号化するなどの方法がある。

【0068】次に図6を用いて第三の発明の実施例を説明する。

【0069】準備フェーズとして、第一の発明の実施例の準備フェーズと同様に行なうが、ステップ15にてタグ票フォーマットを次のように定める。このとき、 $e$ と $n$ と投票内容 $x$ と

30 【0070】

$$\text{ハッシュ値 } h(e \| n \| x)$$

【0071】の連結で、数字として $n_c$ より小さくなるようなものをタグ票とする。

【0072】また、タグ票作成フェーズも第一の発明の実施例と同様に行なうが、タグ票作成手段610にて

【0073】

$$t = e \| n \| x \| h(e \| n \| x)$$

【0074】をタグ票として設定する。ここで $x$ は投票者の意見である。

40 【0075】このようにすれば、タグ票生成時に各投票者は自分の意見を盛り込むことになるので、投票フェーズの時に自分の意見を変更することはできない。

【0076】次に図7を用いて第四の発明の実施例を説明する。

【0077】準備フェーズとして、第二の発明の実施例の準備フェーズと同様に行なうが、ステップ15にてタグ票フォーマットを次のように定める。このとき、 $e$ と $n$ と投票内容 $x$ と

【0078】

$$\text{ハッシュ値 } h(e \| n \| x)$$

【0079】の連結で、数字として $n_c$ より小さくなるようなものをタグ票とする。

【0080】また、タグ票作成フェーズも第二の発明の実施例と同様に行うが、タグ票作成手段710にて

【0081】

$$t = e \parallel n \parallel x \parallel h(e \parallel n \parallel x)$$

【0082】をタグ票として設定する。ここで $x$ は投票者の意見である。

【0083】次に図8を用いて第五の発明の実施例を説明する。これは結果公表フェーズに関する。

【0084】次に図8を用いて結果公表フェーズを説明する。第一の発明の実施例、あるいは第三の発明の実施例のように準備フェーズ、タグ票設定フェーズ、投票フェーズを終えているとし、受理票検証手段207を経て受理票とされたものは受理票保持手段811に格納されているものとする。また、各投票者は自分の投票文を投票文保持手段902に保持しているものとする。

【0085】ここで、一方向性関数として、RSA暗号関数を用いる。

【0086】センタ100はまず、一方向性関数生成手段802において、RSA暗号鍵 $n_2$ 、 $e_2$ を生成する。次に受理票変換手段801において、受け取ったすべての受理票とそのタグを $(n_2, e_2)$ で暗号変換を行なう。すなわち、受理票 $V = (v', T)$ に対して、

【0087】

$$V' = (v', T^{e_2 \bmod n_2})$$

【0088】とする。変換された受理票 $v'$ を受理票公表手段208において、公表する。同時に暗号鍵 $(n_2, e_2)$ も公表する。

【0089】各投票者101(i)は受理票一覧読み出し手段911において、変換された受理票一覧及び暗号鍵 $(n_2, e_2)$ を読み出し、検証手段912において自分の投票が票及びタグが一覧に含まれていることを確認する。すなわち、投票文保持手段902に保持している自分の投票文 $V$ を $(n_2, e_2)$ を用いて

【0090】

$$V' = (v', T^{e_2 \bmod n_2})$$

【0091】と計算し、これが変換された受理票一覧に含まれるかどうかを確認する。

【0092】確認できなければ、異議申し立て手段913を用いて異議申し立てを行なう。これについては後で詳細に述べる。センタはどの投票者からも異議申し立てがなければ、変換されていない受理票と集計結果を公表する。

【0093】一方、検証手段912において自分の投票が受理されていないければ、異議申し立て手段913において、自分のタグ票を公表し、それが正当なタグ票であることと、その変換文が集計されていないことを示す。この主張が確認されれば、異議申し立て者の票が受理さ

れていないと処理される。

【0094】このように異議を申し立てれば、異議申し立て者が実際はどの意見を投票したのかを明らかにすることなく、自分の票が受理されなかったことを証明することができる。さらに、異議申し立て時には全体の投票結果は暗号化されたままなので、投票結果に対する異議とは区別され、従来の方式の様に異議申し立て者が投票結果が不満で異議を唱えているのではないことが明らかになる。

10 【0095】図4を参照すると、いずれの実施例で述べたシステムは、通信処理機能を備えたパーソナルコンピュータ等の端末装置(TMU)401と、読み出し専用記憶装置(ROM)402と、ランダムアクセス記憶装置(RAM)403と、乱数発生器(RNG)404と、シグナルプロセッサ(SP)406と、TMU401、ROM402、RAM403、RNG404およびSP406を相互に接続する共通バス405とから構成される。

【0096】RNG404は乱数をSP406の指令により発生する。これはセンタ100が定数設定の時に用い、また、各投票者101(i)の乱数発生器として用いる。RAM407にはセンタ100の場合、定数保持手段202あるいは秘密情報保持手段201になる。秘密情報はTMUから必要に応じてRAMに格納するようにしてもよい。ROM407には投票者サブシステム101(i)の場合、定数保持手段302、乱数保持器309などになる。ROM内に格納されたプログラムに基づいて、上述の動作を実現する。RAM403はこれらのステップの実行中に計算途中結果等を一時的に記憶するために用いられる。

【0097】また、システム100、101(i)は汎用電子計算機等のデータ処理装置やICカードであってもよい。

【0098】

【発明の効果】以上詳細に説明したように、本発明を用いれば、投票者が自分が何に投票したかを他の投票者に知られることなく不正集計に対して異議申し立てをオープンにでき、同一投票者が2つ以上の選択肢に投票することを検出でき、かつこの検出機構を第三者に悪用されない無記名電子投票装置において、選択肢の数によらず処理量・通信量が一定で、従来方式の最小値(選択肢の数が2の場合)より小さい効率の良い電子投票装置が実現できる。本電子投票装置においては選択肢をあらかじめ定める必要がなく、自由記入式のアンケートにも容易に適用できる。

【図面の簡単な説明】

【図1】第一の発明の電子投票装置の一実施例を示すブロック図。

【図2】無記名電子投票システムを示す図。

【図3】準備フェーズの例を示す図。



11

【図4】第一から第五の発明の実施例に用いるシステムの例。

【図5】第二の発明の電子投票装置の位置実施例を示すブロック図。

【図6】第三の発明の電子投票装置の一実施例を示すブロック図。

【図7】第四の発明の電子投票装置の一実施例を示すブ

ロック図。

【図8】第五の発明の電子投票装置の一実施例を示すブロック図。

【符号の説明】

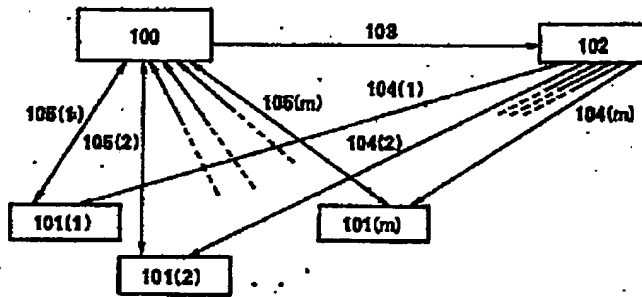
100 選挙管理センタ

101(i) 投票者サブシステム

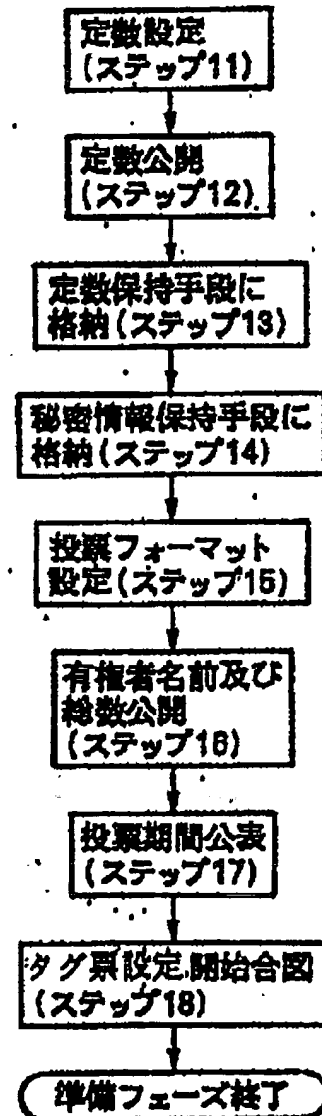
102 電子掲示板

12

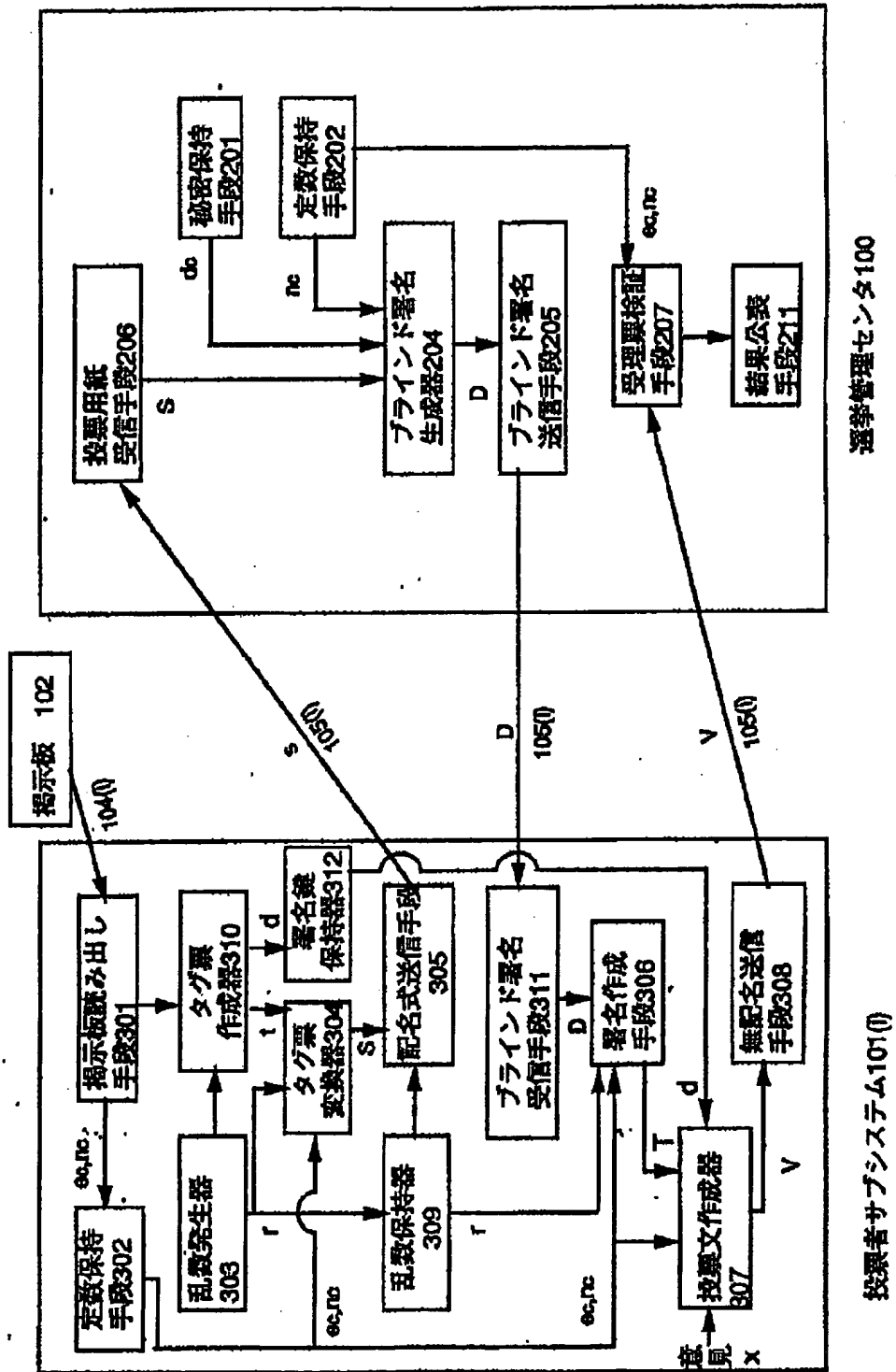
【図2】



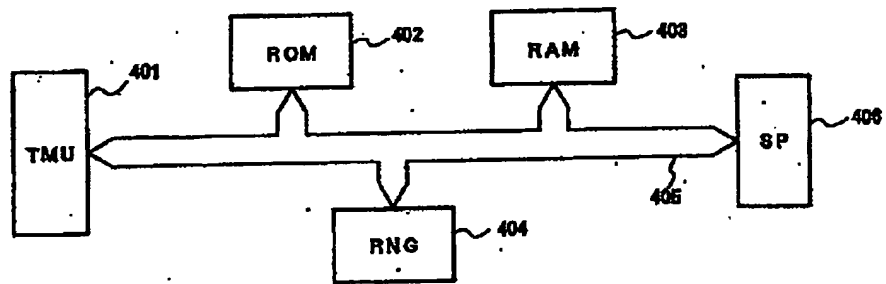
【図3】



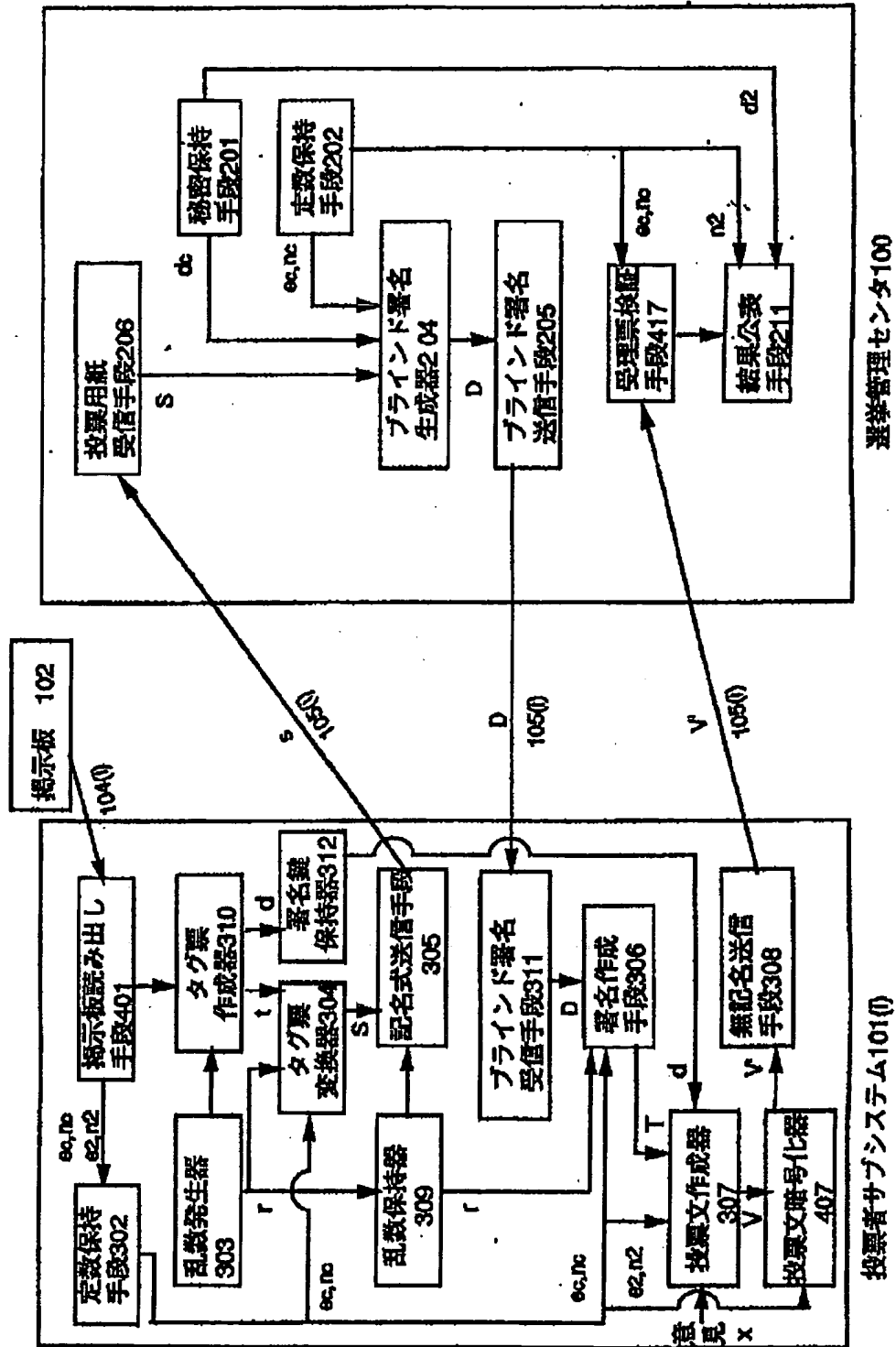
【図1】



【図4】

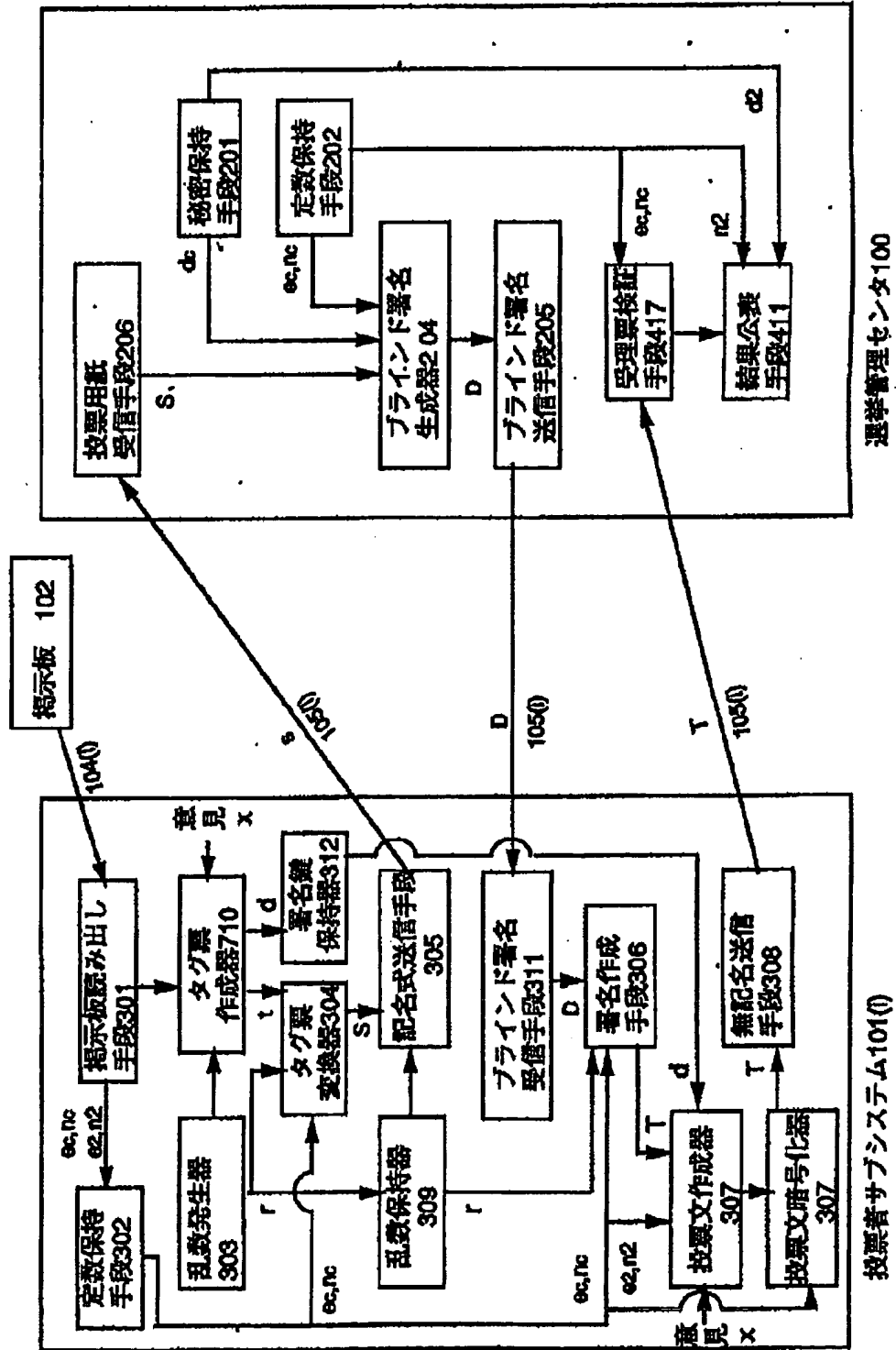


【図5】





【図7】



【図8】

